


# WIZZIT
AUTHENTICATOR

# WIZZIT Authenticator

## Security – Back to basics

In order to manage the current security issues and make sure we have a unified customer experience. We need to go back to fundamental principles that made the initial authentication of transactions on ATM and PIN and apply this to the digital world.

Customers have different user security Journeys for each channel that they use in order to essentially authorise a transaction or approve a debit to a customer account.

With the adoption of the PSD2 framework that has a requirement for strong authentication is expected to further confuse the end customer.

If we go back to basics and adopt the security principle of something you have and something you know being the card and the PIN, and apply this principle to the Mobile phone and the WIZZIT PIN – the customer now has a standard authentication method across both physical and digital channels.

| BANK ENVIRONMENT | | WIZZIT AUTHENTICATOR | |
|---|---|---|---|
| | CURRENT MODEL | FUTURE MODEL | PATH TO GET THERE |
| ATM TRANSACTIONS   | PIN | PIN on ATM | In Place |
| POINT OF SALE  | PIN | PIN on POS | In Place |
| CALL CENTRE  | QUESTIONS & VOICE BIOMETRIC | PIN on CHAT | Simple API from Call Centre to WIZZIT AUTHENTICATOR |
| 3D SECURE   | OTP- Or In app push, password | PIN on CHAT | Route the current OTP Traffic to the WIZZIT AUTHENTICATOR API |
| INTERNET BANKING  | OTP, Fingerprint, Password | PIN on CHAT | Route the current log-on to the WIZZIT AUTHENTICATOR API |